Claims

1. A security server that operates to conditionally enable establishment of a secure interprocess communications session between designated application program instances, said security server comprising:

a) a policy database storing a plurality of policy rules that collectively define the mutual authentication and authorization requirements for establishing a interprocess communications session between first and second application instances; and

b) a security controller interoperative with an operating system that includes an application call interface operative to enable establishment of said interprocess communications session, said security controller being operative to receive predetermined authentication and authorization information from said operating system in connection with a predetermined application call request to establish said interprocess communications session, said security controller being further operative to evaluate said predetermined application call request and said predetermined authentication and authorization information against said plurality of policy rules to conditionally permit the establishment of said interprocess communications session with respect to said first and second application instances.

2. The security server of Claim 1 wherein said security controller is operative to establish a session key that defines a unique encryption of communications data transferred through said communications session between said first and second application instances.

3. The security server of Claim 2 wherein said security controller is operative to evaluate said predetermined application call request and said predetermined authentication and authorization information against said plurality of policy rules to selectively control establishment of said session key with respect to said first and second application instances.

4. The security server of Claim 3 wherein said security controller is operative to provide said session key to said operating system to enable said unique encryption communications data.

5. The security server of Claim 4 wherein said first and second application instances are executed on a common host computer system.

6. The security server of Claim 1 wherein wherein said security server is coupleable to said operating system through a network communications connection.

7. An interprocess communications security system enabling secure communications sessions to be established between designated application instances, said interprocess communications security system comprising:

a) a first computer system coupleable to a communications network, wherein said first computer system includes a first operating system operative to support execution of a first application instance by said first computer system, said first operating system including a first policy enforcement module operative to qualify predetermined communications calls made between said first application instance and said first operating system;

b) a second computer system coupleable to a communications network, wherein said second computer system includes a second operating system operative to support execution of a second application instance by said second computer system, said second operating system including a second policy enforcement module operative to qualify predetermined communications calls made between said second application instance and said second operating system; and

c) a security appliance coupleable to said first and second computer systems through said communications network, said security appliance being interoperable with said first and second policy enforcement modules to mutually authenticate said first and second application instances to conditionally conduct interprocess communications.

8. The interprocess communications security system of Claim 7 wherein said security appliance is further interoperable with said first and second policy enforcement modules to enable encryption processing of interprocess communications exchanged between said first and second application instances.

9. The interprocess communications security system of Claim 8 wherein said security appliance is operative to determine an encryption token with respect to the mutual authentication of said first and second application instances, to provide said encryption token to said first and second policy enforcement modules

for use in encrypting processing of interprocess communications exchanged between said first and second application instances.

10. The interprocess communications security system of Claim 9 wherein said security appliance includes a policy database storing a plurality of policy rules and a control program operative to evaluate said plurality of policy rules, wherein said first and second policy enforcement modules are operative to provide said security appliance with predetermined information associated with said first and second application instances in connection with a predetermined communications call request by said first application instance to establish interprocess communications with said second application instance, and wherein said security appliance conditionally enables establishment of an interprocess communications session between said first and second application programs in response to said predetermined communications call request dependent on an evaluation of said plurality of policy rules with respect to said predetermined information.

11. The interprocess communications security system of Claim 10 wherein said predetermined information includes a secure identification of said first and second application instances and wherein said secure identification is used to mutually authenticate said first and second application instances.

12. The interprocess communications security system of Claim 11 wherein said security appliance includes a signature database storing a plurality of secure signatures, wherein said predetermined information includes secure signatures for said first and second application instances, and wherein said security appliance

is operative to compare the secure signatures of said first and second application instances to said plurality of secure signatures.

13. An interprocess communications security system enabling secure trust relationships to be established at any level down to the level of individual application instances as executed on respective host computer systems interconnected by a communications network, said system comprising:

a) a first host computer operative to support execution of a first application instance within a first predefined process context;

b) a second host computer system operative to support execution of a second application instance in a second predefined process context;

c) control means, provided with respect to said first and second host computer systems, for establishing communications channels between said first and second host computer systems including a predetermined communications channel conducting communications between said first and second predefined process contexts, said control means being responsive to predetermined information identified with said first and second predefined process contexts to determine a session encryption key for use exclusively in encryption processing of communications conducted through said predetermined communications channel.

14. The interprocess communications security system of Claim 13 wherein said predetermined information identified with said first and second predefined process contexts includes secure identifications of said first and second application instances.

15. The interprocess communications security system of Claim 14 wherein said control means provides for a policy-based evaluation of said predetermined information identified with said first and second process contexts.

16. The interprocess communications security system of Claim 15 wherein said first and second predefined process contexts are established on said first and second computer systems by first and second operating systems and wherein said control means includes policy enforcement means implemented in combination with said first and second operating systems to conditionally enable establishment of said predetermined communications channel subject to said policy-based evaluation.

17. The interprocess communications security system of Claim 16 wherein said control means includes a security server computer system operable to receive said predetermined information, to perform said policy-based evaluation, and to control said policy enforcement means in conditionally enabling establishment of said predetermined communications channel.

18. The interprocess communications security system of Claim 17 wherein said security server computer system determines said session encryption key.

19. The interprocess communications security system of Claim 18 wherein said session encryption key is provided to said policy enforcement means to perform encryption processing for communications conducted between said first and second process contexts.

20. A method of binding application execution contexts on network connected computer systems through a secure communications channel, said method comprising the steps of:

a) first enabling execution of a first application instance on a first computer system dependent on a first security assessment of a first application context within which said first application instance is executable;

b) second enabling execution of a second application instance on a second computer system dependent on a second security assessment of a second application context within which said second application instance is executable;

c) third enabling communications between said first and second application instances dependent on a mutual security assessment of said first and second application contexts; and

d) selectively establishing an encrypted communications channel between said first and second application instances wherein use of said encrypted communications channel is enabled by a session key shared between said first and second application contexts.

21. The method of Claim 20 wherein data, representative of said first and second application contexts, is communicated to a security server, said method

further comprising the step of evaluating said data to perform said first, second, and mutual assessments of said first and second application contexts.

22. The method of Claim 21 further comprising the step of determining, by said security server, said session key.

23. The method of Claim 22 further comprising the step of communicating said session key from said security server to said first and second application contexts, wherein communications through said encrypted communications channel are transferred directly, relative to said security server, between said first and second application contexts.

24. A method of securely binding communications between processes, wherein application instances, within respective processes, are executed on computer systems in process execution contexts, said method comprising the steps of:

a) intercepting communications between first and second predetermined process execution contexts; and

b) encrypting intercepted network communication transmissions and decrypting intercepted communication receptions utilizing an encryption key uniquely established based on an evaluation of authorization and authentication information descriptive of said first and second predetermined process execution contexts.

25. The method of Claim 24 wherein sets of one or more related processes are executed in process execution contexts, and wherein said step of intercepting

communications includes the steps of identifying said first and second predetermined process execution contexts as a unique communication session and of obtaining a session encryption key specific to said secure communications session for said network communication.

26. The method of Claim 25 wherein said session encryption key is unique to said unique communications session.

27. The method of Claim 26 further comprising the step of determining said session encryption key uniquely in connection with the establishment of said unique communications session.

28. The method of Claim 27 further comprising the step of requesting, with respect to said first and second predetermined execution contexts, said session key from a security server.

29. The method of Claim 28 wherein said security server is an independent computer system relative to the computer systems providing for the execution of said first and second process execution contexts, wherein said step of requesting provides for the transfer of predetermined authorization and authentication information descriptive of said first and second execution contexts, including secure identifications of first and second application instances, to said security server, and wherein said security server performs said step of determining dependent on said predetermined authorization and authentication information.

30. A method of securely binding process communications, said method comprising the steps of:

a) intercepting, on first and second host computer systems, communications data directed between first and second application instances executed respectively on said first and second host computers; and

b) transferring the intercepted communications data, in encrypted form, between said first and second application instances, wherein the intercepted communications data is encrypted using an encryption key determined specific to said first and second application instances.

31. The method of Claim 30 wherein said step of intercepting is performed transparently with respect to said first and second application instances.

32. The method of Claim 31 further comprising the step of requesting said encryption key from a security server computer system separate from said first and second host computer systems, said step of requesting including the steps of communicating predetermined identification data, including an identification of said first and second application instances, to said security server computer system and of selectively receiving said encryption key.

33. The method of Claim 32 further comprising the step of determining, by said security server computer system, said encryption key specific to said predetermined identification data.

34. A system of securing communications between application instances executable on respective host computer systems, said system comprising:

a) first and second computer systems operable to execute respective pluralities of application instances; and

b) first and second secure communications modules respectively executable by said first and second computer systems, said first and second secure communications modules being operative to identify discrete communications sessions between specific pairs of application instances among said pluralities of application instances and establish encrypted communications channels between said first and second secure communications modules for respective communication sessions.

35. The system of Claim 34 further comprising a security server computer system operative to provide a distinct session encryption key to said first and second secure communications modules for respective communication sessions.

36. The system of Claim 35 wherein said security server computer system includes a policy database, wherein said first and second secure communications modules are coupleable to said security server computer system to provide predetermined request data with respect to a predetermined communication session, wherein said server computer system is operative to evaluate said predetermined request data against said policy database and selectively return said distinct session encryption key for said predetermined communication session.

37. The system of Claim 36 wherein said predetermined request data includes first request data including a first identification of a first application instance and second request data including a second identification of said second application instance.

38. The system of Claim 37 wherein said first and second identifications are secure identifications.

39. The system of Claim 38 wherein said predetermined request data identifies provides user identification, user authentication, and application instance identification information for said first and second application instances.

40. A system for controlling the execution and mutual communication between remotely executing programs, said system comprising:

a) a first control program executable by a first computer system operative, by execution of a first operating system, to support execution of a first predetermined program, said first control program operative to process first predetermined data transfers between said first predetermined program and said first operating system;

b) a second control program executable by a second computer system operative, by execution of a second operating system, to support execution of a second predetermined program, said second control program operative to process second predetermined data transfers between said second predetermined program and said second operating system; and

c) a security server coupleable to said first and second predetermined programs to selectively enable processing of said first and second predetermined data transfers dependent on security values evaluated by said security server with respect to said first and second predetermined programs.

41. The system of Claim 40 wherein said first and second control programs are further respectively operative to provide first and second sets of security values, corresponding respectively to said first and second predetermined programs, to said security server.

42. The system of Claim 41 wherein said security server is operative to enable processing of said first and second predetermined data transfers where said first and second predetermined data transfers provide for the communication of data between said first and second predetermined programs dependent on the mutual evaluation of said first and second sets of security values.